

1  
2  
3 **UNITED STATES DISTRICT COURT**  
4 **NORTHERN DISTRICT OF CALIFORNIA**  
5

6 **UNITED STATES OF AMERICA,**

7 Plaintiff,

8 vs.

9 **MARTHA JULIA MAFFEI,**

10 Defendant.

CASE NO. 18-cr-00174-YGR-1

**ORDER GRANTING MOTION TO SUPPRESS  
EVIDENCE**

Re: Dkt. No. 21

11 Defendant has been charged with a twenty-seven count indictment related to an alleged  
12 scheme to defraud, including charges of conspiracy to commit mail and wire fraud in violation of  
13 18 U.S.C. § 1349, mail fraud in violation of 18 U.S.C. § 1341, wire fraud in violation of 18 U.S.C.  
14 § 1343, laundering in monetary instruments in violation of 18 U.S.C. § 1956, and engaging in  
15 monetary transactions in property derived from specified unlawful activity in violation of 18  
16 U.S.C. § 1957.<sup>1</sup> (Dkt. No. 9 (“Indictment”).) The Court considers defendant’s motion to suppress  
17 her statement of the passcode to her cellphone (described as evidence item SIRGM2 and seized by  
18 law enforcement agents on April 12, 2018), the resulting search of that device, and all evidence  
19 subsequently derived from that search. (Dkt. No. 21 (“Motion”).)

20 Having carefully considered the motion and the papers submitted, as well as oral argument  
21 from counsel on February 28, 2019, and for the reasons set forth more fully below, the Court  
22 **GRANTS** defendant’s motion to suppress and excludes from evidence defendant’s statement  
23 regarding her cellphone passcode, the resulting search of her cellphone, and all evidence  
24 subsequently derived from that search, except for use to impeach defendant’s testimony, should  
25 she chose to testify at trial.  
26

27  
28 <sup>1</sup> According to the indictment, defendant’s conduct also subjects her to criminal forfeiture  
upon conviction of violation of 18 U.S.C. §§ 1956, 1957 pursuant to 18 U.S.C. §§ 981(a)(1)(C),  
982(a) and 28 U.S.C. § 246(c). (Indictment ¶¶ 32-35.)

**I. BACKGROUND**

At some point prior to November 2017, the Department of Labor, Office of the Inspector General (“OIG”) opened an investigation into defendant Maffei’s involvement in an alleged scheme to defraud timeshare owners by posing as either timeshare brokers representing potential buyers or Special Agents of the OIG or the Treasury Department and encouraging victims to make various payments via check or money wire (the “Scheme”). (Indictment ¶¶ 10-12.)

During the course of the OIG’s investigation into the Scheme, on November 5, 2017, San Mateo Police Department (“SMPD”) conducted an enforcement stop on a Toyota Camry due to a broken tail light and the driver’s failure to yield to pedestrians in a crosswalk. (*See* SMPD Police Report re: Traffic Stop (“SMPD Report”) at MJM-543.) Defendant, Martha Maffei, was the only passenger in the car, and her husband, Michael Maffei, was the driver. (*Id.* at MJM-544.) After determining that Michael Maffei’s license had expired, the officers conducted an “inventory search” of the vehicle. (*Id.*) The search recovered Oxycodone pills, marijuana, and a purse containing approximately \$11,000 in cash. (*Id.* at MJM-545.) The officers also recovered two Apple iPhone devices from the car. (*Id.*) SMPD arrested defendant, along with her husband, for possession of narcotics for sale, transportation/sales of narcotics, and conspiracy to commit a crime. (SMPD Report at MJM-543.)

Following the arrest on November 5, 2017, SMPD officers went with defendant and her husband to their home to conduct a welfare check regarding the couple’s two children. (*Id.* at MJM-546.) During the visit, the officers observed “(in plain view) indicia to additional narcotic and federal crimes.” (*Id.*) That evening, SMPD officers applied for a search warrant for the Maffei residence, which a judge of the San Mateo Superior Court signed the next day, November 6, 2017. (*See* San Mateo Search Warrant (“SM Warrant”) at MJM-557.) The warrant authorized the search for and seizure of various narcotics and paraphernalia related to drug sales as well as cellphones and other digital devices. (*Id.* at MJM-560.) The warrant also addressed the two iPhones seized during the November 5 traffic stop. (*Id.* at MJM-561.) Specifically, the warrant provided for a forensic examination of the cellphones, as well as a physical or “finger search” of the phones, “includ[ing] the owner providing officers with the device’s passcodes, or placing

1 his/her fingerprint to the device's screen in order to unlock the [phone]." (*Id.* at MJM-562.)

2 Defendant initially refused to provide the passcode for her locked cellphone. (*See*  
3 Affidavit in Support of Federal Criminal Complaint ("Aff. in Sup. Fed. Compl.") ¶ 65.) On  
4 November 6, 2017, after her release, defendant provided two possible passcodes for her cellphone,  
5 but officers did not immediately attempt to unlock the phone. (*Id.*) When a forensic examiner for  
6 SMPD examined the phone on November 15, 2017, she reported that the iPhone was "already in  
7 set up mode[.]" which indicated that someone had "wiped" the device. (*See* SMPD Supplemental  
8 Report ("SMPD Suppl. Report") at MJM-5325.) The examiner then used Cellebrite to extract the  
9 data stored on the phone's sim card. (*Id.*)

10 Shortly after defendant's arrest, SMPD referred her case to federal authorities, who,  
11 between December 12, 2017 and February 15, 2018, sought and obtained a series of federal search  
12 warrants related to the OIG's investigation into the Scheme. Special Agent ("SA") Chris Collins  
13 of the OIG drafted each of the applications.

14 First, on December 12, 2017, Magistrate Judge Laporte signed search warrant number 17-  
15 71650, which authorized a search of defendant's cellphone—the same iPhone that officers seized  
16 during the traffic stop and the forensic officer subsequently examined. (*See* N.D. Cal. Search  
17 Warrant No. 17-71650 ("CAND Warrant -650") at MJM-5389.) Once Judge Laporte issued the  
18 warrant, OIG agents obtained custody of the phone from SMPD and "discovered that all of the  
19 contents on [defendant's] iPhone appeared to have been remotely erased, and no information was  
20 able to be recovered." (Aff. in Sup. Fed. Compl. ¶¶ 65-66.) Judge Laporte also signed a second  
21 warrant on December 12, 2017, numbered 17-71651, which authorized the search of Google email  
22 content for Google accounts allegedly associated with the Scheme. (*See* N.D. Cal. Search Warrant  
23 No. 17-71651 ("CAND Warrant -651") at MJM-5422.) The warrant provided for the search of  
24 four accounts, including marthamaffei@gmail.com. (*Id.* at MJM-5423.) Google provided the  
25 search warrant returns on January 4, 2018. (Aff. in Sup. Fed. Compl. ¶ 8.)

26 Judge Laporte signed a third search warrant, number 17-71688, on December 29, 2017 for  
27 the four digital devices—two Apple MacBooks and two iPads—that SMPD seized from  
28 defendant's home on November 6, 2017. (*See* N.D. Cal. Search Warrant No. 17-71688 ("CAND

Warrant -688”) at MJM-5355.) Three of these devices were encrypted and, because the federal investigators did not have the passcodes, they did not analyze them. (Aff. in Sup. Fed. Compl. ¶ 7.) The agents were able to access the fourth device but determined the contents were not responsive to the warrant. (*Id.*)

Finally, on February 15, 2018, Magistrate Judge Westmore signed search warrant number 18-70191, which authorized a search by Facebook for information associated with defendant’s account as well as another Facebook account of interest to investigators. (*See* N.D. Cal. Search Warrant No. 18-70191 (“CAND Warrant -191”) at MJM-5328.)

On April 9, 2018, SA Collins filed an affidavit in support of a search warrant, arrest warrant, and criminal complaint. (Aff. in Sup. Fed. Compl. ¶ 2.) The application sought authorization for a search of defendant’s apartment, car, and “any digital devices belonging to [defendant], such as a computer and mobile phones, which are recovered pursuant to the searches [sic] and/or arrest of [defendant] (“SUBJECT DEVICES”).” (*Id.* ¶ 3.)

Notably, the search warrant application explicitly requested authority to “compel [defendant] to provide a biometric key (facial recognition or thumbprint) to unlock any SUBJECT DEVICE recovered during the execution of the search warrants.” (*Id.* ¶ 90; *see also id.* ¶ 3 (“The affidavit also seeks to require [defendant] to provide a fingerprint or facial recognition to unlock any SUBJECT DEVICES recovered during the execution of the warrants.”) Although SA Collins mentioned elsewhere in the warrant application that “Apple iPhones require either a multi-digit passcode or a biometric key” and “[u]pon successful opening of the phone, law enforcement will adjust the passcode . . . [,]” the application itself sought only the authority to compel defendant to provide a *biometric key* and did not request permission or authority from the magistrate to compel defendant to provide her passcode, whether through oral statements or other means. (*Id.* ¶¶ 89, 90.) Later that day, Judge Laporte signed the search and arrest warrants as well as the criminal complaint. (*Id.* at MJM-6038.)

OIG agents executed the federal search and arrest warrants on April 12, 2018 with the assistance of SMPD. (*See* OIG Memo to File by Ferrer (“Ferrer OIG Memo”) at MJM-843.) When OIG agents and SMPD officers arrived at defendant’s home to execute the warrants, they

1 quickly escorted her out of her residence, handcuffed and searched her, and reportedly advised her  
2 of her *Miranda* rights. (*Id.*) Shortly thereafter, SA Collins and SA Ana Ptaszek transported  
3 defendant to the federal courthouse in San Francisco. (*Id.* at MJM-844.)

4 During the drive to the courthouse, SA Collins told defendant that “he was not going to ask  
5 her any questions,” and that “he hoped she would cooperate in the investigation” and “explained  
6 that, in general, when people cooperate it helps their situation.” (*See* OIG Memo to File by  
7 Collins (“Collins OIG Memo”) at MJM 849.) Defendant did not respond other than to request to  
8 contact Paula Canny, the private attorney who had represented defendant in her state case. (*Id.*)  
9 SA Collins attempted to call Ms. Canny from his cell phone and left her a voicemail indicating  
10 that defendant “had been arrested on a federal warrant for money laundering.” (*Id.*) After SA  
11 Collins arrived at the federal courthouse and transferred defendant to the custody of the U.S.  
12 Marshals, Ms. Canny returned his call and informed him that she could not represent defendant at  
13 her initial appearance due to a recent surgery. (*Id.*)

14 Approximately four hours after the agents first executed the federal search and arrest  
15 warrants on the morning of April 12, defendant made her initial appearance, during which the  
16 court provisionally appointed Assistant Federal Public Defender Jodi Linker to represent her. (*See*  
17 Dkt. No. 3.) Following the appearance hearing, the court remanded defendant into custody. (*Id.*)  
18 An hour later, SA Collins and SA Ptaszek visited defendant in the U.S. Marshals holding cell on  
19 the twentieth floor of the San Francisco federal courthouse. (Collins OIG Memo at MJM-849.)  
20 During this encounter, SA Collins “informed [defendant] that he was there to get the passcodes for  
21 the phones.” Defendant then provided the passcode for evidence item SIRGM2, an Apple iPhone  
22 device. (*Id.* at MJM-850.) “SA Collins verified that the passcode worked.” (*Id.*) SA Collins also  
23 showed defendant photos of two other devices, also Apple iPhones found in defendant’s residence,  
24 and defendant replied that cellphones belong to her son and that she did not know the passcodes.  
25 (*Id.*) SA Collins then “thanked [defendant] for her cooperation.” (*Id.*)

## 26 II. ANALYSIS

27 Defendant brings the instant motion on the grounds that in obtaining her cellphone  
28

passcode, law enforcement violated her Fourth, Fifth, and Sixth Amendment rights. (*See* Motion.) In its opposition, the government represents that although it does not intend to introduce the evidence at issue in this motion in its case-in-chief, it does reserve its right to use the evidence to impeach defendant’s testimony at trial. (Dkt. No. 26 (“Opp.”) at 1.) Specifically, the government argues that because defendant provided her passcode voluntarily, the government may use the statement and the evidence obtained by the resulting search to impeach defendant’s testimony, even if law enforcement obtained that statement in violation of defendant’s *Miranda* rights. (*Id.* at 3-4.) The government also asserts that because it does not intend to use the evidence in its case-in-chief, defendant’s motion to suppress is moot. (*See id.*) The government does not further address defendant’s Fourth, Fifth, and Sixth Amendment arguments. (*See id.*)

In light of its opposition, during oral argument on February 28, 2019, the Court asked the government whether it conceded that law enforcement’s conduct violated defendant’s rights and that it could not use the evidence affirmatively. The government would not so concede and maintained, for the first time, that even if law enforcement did violate defendant’s rights, the inevitable discovery rule would apply and so the Court should not suppress the evidence. Accordingly, the Court evaluates each of defendant’s arguments for suppression in turn.

#### **A. The Fourth Amendment**

The Fourth Amendment protects “[t]he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. It also generally requires law enforcement officers to obtain a warrant before they may search the digital data on a cellphone, even when officers seize that cellphone incident to a lawful arrest. *See Riley v. California*, 134 S. Ct. 2473, 2493 (2014). Here, the government obtained a search warrant authorizing the search and seizure of digital devices, including the cellphone at issue, prior to confiscating the cellphone, requesting the passcode, and searching the phone’s contents. (*See* Aff. in Sup. Fed. Compl. ¶¶ 78-90.) The warrant application specifically requested the “authority to compel [defendant] to provide a *biometric key* (facial recognition or thumbprint) to unlock” the cellphone at issue. (*Id.* ¶ 90 (emphasis supplied).) As defendant does not challenge the validity of the warrant for lack of probable cause or insufficient particularity, the Court turns to whether SA

Collins exceeded the scope of the warrant when he obtained from defendant the *multidigit passcode* to her cellphone, rather than a biometric key.

If the “scope of [a] search exceeds that permitted by the terms of a validly issued warrant . . . [the search and any] subsequent seizure [are] unconstitutional.” *Horton v. California*, 496 U.S. 128, 140 (1990). In deciding whether a search exceeded its lawful scope, a court may consider “both the purpose disclosed in the application for a warrant’s issuance and the manner of its execution.” *United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978). Whether a search exceeds the scope of the relevant search warrant requires an objective inquiry that looks at the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search. *United States v. Hitchcock*, 286 F.3d 1064, 1071 (9th Cir. 2002), *superseded on other grounds by United States v. Hitchcock*, 298 F.3d 1021 (9th Cir. 2002).

The text of the application at issue here requested, and therefore the signed warrant provided, only the “authority to compel [defendant] to provide a biometric key (facial recognition or thumbprint) to unlock any” Subject Device “in order to open the phone in a law enforcement controlled setting.” (Aff. in Sup. Fed. Compl. ¶ 90.) Notably, elsewhere in the search warrant application, the agent explained that “Apple iPhones require *either* a multi-digit passcode *or* a biometric key” and that “[u]pon successful opening of the phone, law enforcement will adjust the *passcode* to allow for successful opening of the phone out of the presence of [defendant.]” (*Id.* ¶¶ 89, 90.) Yet, the agent only sought the authority to compel defendant to provide a biometric key and *did not* request permission or authority to compel defendant to provide her multidigit passcode. (*Id.* ¶¶ 3, 90.)

Although neither the Supreme Court nor the Ninth Circuit have spoken directly on the relationship between and the interchangeability of a multidigit passcode and a biometric key in decrypting a device seized pursuant to a warrant, the Court does not consider the two perfect substitutes in evaluating the scope of the warrant. From a practical standpoint, a passcode and a biometric key serve different functions. Apple iPhone software will often not accept the biometric key and will require the multidigit passcode to unlock the device—for example, when one restarts the device or engages in too many failed attempts to unlock the phone via the biometric key, or if

more than 48 hours have passed since the device was last unlocked using a biometric key. *About Touch ID Advanced Security Technology*, (Sept. 11, 2017) <https://support.apple.com/en-us/HT204587>.<sup>2</sup> More importantly in this context, iPhone software requires the multidigit passcode in order to change or remove the encryption on the device. *Id.* The government seems to have considered this issue and still did not request the authority to compel defendant’s passcode. (*See* Aff. in Sup. Fed. Compl. ¶ 90.) Thus, the Court finds that obtaining defendant’s passcode, rather than a biometric key, constituted materially different conduct for the purposes of determining whether law enforcement exceeded the scope of the warrant.

Additionally, in light of recent developments in this area of law in this District, it seems possible that a magistrate would have denied an application for a warrant authorizing officers to compel defendant’s cellphone *passcode* as violating the Fifth Amendment. *See United States v. Spencer*, No. 17-cv-00259-CRB-1, 2018 WL 1964588, at \*2 (N.D. Cal. Apr. 26, 2018) (“For instance, the government could not compel Spencer to state the [cellphone] password itself, whether orally or in writing.”) (citing *Doe v. United States*, 487 U.S. 201, 210 n. 9 (1988)) (alteration supplied); *see also supra* III.B.1. Moreover, SA Collins, the author of the warrant application, seems to have understood the multidigit passcode and biometric key as distinct methods of opening the device and therefore could have drafted a warrant application requesting authority to compel a multidigit passcode, and yet did not. (*See id.* ¶ 89 (“I know Apple iPhones require either a multi-digit passcode or a biometric key . . . in order to open the phone.”).)

For these reasons, the Court finds that by visiting defendant in the U.S. Marshals facility and “inform[ing] [her] that he was there to get the passcodes for the phones” SA Collins exceeded the scope of the warrant in violation of the Fourth Amendment.

\\

\\

---

<sup>2</sup> *See also Search of a Residence in Oakland, California*, Case No. 19-CV-70053-KAW, 2019 WL 176937 (N.D. Cal. Jan. 10, 2019), at \*3 (noting that “there are times when the device will not accept the biometric feature and require the user to type in the passcode to unlock the device”).



## 1                    **B. The Fifth Amendment**

2                    Defendant asserts two grounds rooted in the Fifth Amendment for suppressing her  
3 statement regarding the passcode to her cellphone, the resulting search of her phone, and all  
4 evidence subsequently derived from that search, namely that SA Collins: (1) compelled the  
5 statement in violation of the Fifth Amendment; and (2) violated defendant’s *Miranda* rights by  
6 attempting to obtain her passcode after she had invoked her right to counsel.

### 7                    1. Compelled Testimony in Violation of the Fifth Amendment

8                    The Fifth Amendment provides that “no person . . . shall be compelled in any criminal case  
9 to be a witness against himself.” U.S. Const. amend. V. This privilege extends not only “to  
10 answers that would in themselves support a conviction . . . but likewise embraces those which  
11 would furnish a link in the chain of evidence needed to prosecute the claimant.” *Hoffman v.*  
12 *United States*, 341 U.S. 479, 486 (1951). To prove a violation of this privilege, an individual must  
13 establish (a) self-incrimination (b) by way of testimonial communication and (c) compulsion.  
14 *United States v. Hubbell*, 530 U.S. 27, 34-38 (2000); *Hiibel v. Sixth Jud. Dist. Ct. of Nev.*,  
15 *Humboldt Cnty.*, 542 U.S. 177, 189 (2004). The Court discusses each.

#### 16                    a. *First Prong: Self-Incrimination*

17                    The Fifth Amendment “protects against any disclosures which the witness reasonably  
18 believes could be used in a criminal prosecution or could lead to other evidence that might be so  
19 used.” *Kastigar v. United States*, 406 U.S. 441, 445 (1972); *see also Doe v. United States*, 487  
20 U.S. 201, 213 (1988) (noting that the Fifth Amendment is intended to “spare the accused from  
21 having to reveal, directly or indirectly, his knowledge of the facts relating him to the offense”).  
22 Providing information that could lead to other evidence that might be used in a criminal  
23 prosecution similarly qualifies as “self-incriminating.” *See Fisher v. United States*, 425 U.S. 391,  
24 410 (1976). Defendant’s provision of the passcode to her cell phone so qualifies as information on  
25 the phone may be incriminating. *See id.*; *Spencer*, 2018 WL 1964588, at \*2 (finding that the act  
26 of requiring a defendant to aid in decryption of electronic devices “would potentially be  
27 incriminating because having that ability makes it more likely that [the defendant] encrypted the  
28 devices, which in turn makes it more likely that he himself put the sought-after material on the

devices”).<sup>3</sup>

b. *Second Prong: Testimonial Communication*

The “vast majority of verbal statements . . . will be testimonial” because “[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts. Whenever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the ‘trilemma’ of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component.” *Pennsylvania v. Muniz*, 496 U.S. 582, 597 (1990) (citing *Doe*, 487 U.S. at 213). Additionally, the mere “act of producing evidence . . . has communicative aspects of its own” that may qualify as testimonial, *Fisher*, 425 U.S. at 410, especially where such an act requires an individual to call upon the contents of his or her own mind. *Hubbell*, 530 U.S. at 43 (citing *Curcio v. United States*, 354 U.S. 118, 128 (1957)); *see also Doe*, 487 U.S., at 210, n. 9 (stating, in dicta, that unlike forcing someone to surrender “a key to a strongbox,” compelling someone to reveal the combination to a wall safe constitutes a testimonial communication within the meaning of the Fifth Amendment).

Although neither the Supreme Court nor the Ninth Circuit have addressed whether aiding in decryption of an electronic device, through provision of a biometric key, alphanumeric passcode, or otherwise, qualifies as a testimonial communication, provision of a passcode bears a striking similarity to “telling an inquisitor the combination to a wall safe.” *See Hubbell*, 530 U.S. at 43 (citing *Doe*, 487 U.S. at 210, n. 9). Of the courts of appeal, only the Eleventh Circuit has addressed the decryption issue directly. *See In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1345 (11th Cir. 2012). Therein, the court relied on the Supreme Court’s decisions in *Fisher*, *Doe*, and *Hubbell* to determine that “the decryption and production of

---

<sup>3</sup> *See also Search of a Residence in Oakland, California*, 2019 WL 176937, at \*3; *In re Application for a Search Warrant*, 236 F.Supp.3d 1066, 1073 (N.D. Ill. 2017) (observing that by providing a biometric passcode to a cellphone, “a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents”).

1 the contents of  
2 . . . hard drives is testimonial in character.” *Id.* at 1345 (“Requiring Doe to use a decryption  
3 password is most certainly more akin to requiring the production of a combination because both  
4 demand the use of the contents of the mind, and the production is accompanied by the implied  
5 factual statements [regarding the defendant’s role in placing contents on and encrypting the hard  
6 drive] noted above that could prove to be incriminatory.”) Defendant’s provision of her cellphone  
7 passcode similarly demands the use of the contents of her mind and implies factual statements,  
8 including which of the three seized cellphones belonged to her and that she had control over or a  
9 relatively significant connection to the cellphone identified as evidence item SIRGM2. Therefore,  
10 defendant’s statement constitutes a testimonial communication.<sup>4 5</sup> *See id.*; *see also In re*  
11 *Application for a Search Warrant*, 236 F.Supp.3d at 1073 (determining that provision of a  
12 fingerprint key to access an iPhone via Apple’s biometric security system qualifies as testimonial  
13

---

14 <sup>4</sup> Additionally, the privacy concerns related to the immense storage capacity of the modern  
15 cellphone articulated by the Supreme Court in *Riley* weigh in favor of this finding. *See Riley*, 573  
16 U.S. at 393-95 (“First, a cell phone collects in one place many distinct types of information—an  
17 address, a note, a prescription, a bank statement, a video—that reveal much more in combination  
18 than any isolated record. Second, a cell phone’s capacity allows even just one type of information  
19 to convey far more than previously possible. The sum of an individual’s private life can be  
20 reconstructed through a thousand photographs labeled with dates, locations, and descriptions; . . .  
21 Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person  
22 might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a  
23 record of all his communications with Mr. Jones for the past several months, as would routinely be  
24 kept on a phone. Finally, there is an element of pervasiveness that characterizes cell phones but  
25 not physical records.”).

26 <sup>5</sup> Although the government does not raise the issue, the Court notes that the foregone  
27 conclusion doctrine does not apply as the government has not alleged, and the facts do not  
28 suggest, that the government already knew that defendant had the passcode to the cellphone such  
that her provision thereof “add[ed] little or nothing to the sum total of the Government’s  
information[.]” *In re Grand Jury Subpoena, Dated April 18, 2003*, 383 F.3d 905, 910 (9th Cir.  
2004); *c.f. Spencer*, 2018 WL 1964588, at \* 3 (holding that a defendant’s ability to decrypt hard  
drives was a foregone conclusion where device was found in defendant’s exclusive residence,  
defendant conceded that he owned the other two devices found therein, a phone and a laptop, and  
had already provided the login passwords for both, and defendant conceded that he purchase and  
encrypted an external hard drive matching the description of the one found by the government). In  
fact, SA Collins presented defendant with two other iPhones as well, for which she did not have  
the passcodes. (Collins OIG Memo at MJM-850.)

because it constitutes “*producing* the contents on the phone” and explaining that “[w]ith a touch of the finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents”); *c.f. Matter of Search of [Redacted] Washington, District of Columbia*, 317 F. Supp.3d 523, 538 (D.D.C. 2018) (finding that because the collection process for a biometric feature “requires no . . . cognitive exertion by the [s]ubject” and “will not require the [s]ubject to make any use of the contents of his mind[,]” compelled use of a biometric feature to decrypt a device does not constitute a testimonial communication).

*c. Third Prong: Compulsion*

In order to determine whether testimony has been “compelled,” courts look to “whether, considering the totality of the circumstances, the free will of the witness was overborne.” *See United States v. Anderson*, 79 F.3d 1522, 1526 (9th Cir. 1996) (quoting *United States v. Washington*, 431 U.S. 181, 188 (1977)). Said differently, the issue is whether a defendant *voluntarily* provided the information. Generally, the Court considers whether a statement is voluntary in the context of the coerciveness of an interrogation.

Defendant has not alleged, nor do the facts suggest, that her free will was “overborne” by the custodial context in which SA Collins obtained her passcode. Prior to SA Collins’ inquiry regarding the passcode, OIG agents advised defendant of her *Miranda* rights, including her right to remain silent. (*See* Ferrer OIG Memo at MJM-843; *see also* Motion at 11.) The custodial setting in which SA Collins approached defendant for her passcode does not, alone, rise to the level of “threatening to sanction the person unless the constitutional privilege is surrendered[.]” *Anderson*, 79 F.3d at 1527; *c.f. United States v. Sanchez*, 334 F.Supp.3d 1284, 1297 (N.D. Ga. 2018), *appeal docketed*, No. 18-15289 (11th Cir. December 24, 2018) (finding compulsion and therefore violation of the Fifth Amendment where the defendant’s probation officer told him that his refusal to provide the passcodes to his iPhones could result in his arrest for a parole violation); *see also Columbe v. Connecticut*, 367 U.S. 568, 579 (1961) (“Often the place of questioning will have to be a police interrogation room . . .”). Additionally, although SA Collins’ statement on

the way to the courthouse that “he hoped [defendant] would cooperate in the investigation” and explanation that “in general when people cooperate it helps their situation” (Collins OIG Memo at MJM-849) might suggest a slight implication that defendant would receive something in return for cooperating, such appeals are not objectionable if the officer did not promise anything specific. *See Fare v. Michael C.*, 442 U.S. 707, 727 (1979). Moreover, Collins “emphasized that he cannot make any promises or guarantees[.]” (Collins OIG Memo at MJM-849.)

Accordingly, based on its three-prong analysis, the Court finds defendant’s response was not *compelled* in violation the Fifth Amendment. *See United States v. Swacker*, 628 F.2d 1250, 1253 (9th Cir. 1980) (citing *Washington*, 431 U.S. at 189) (holding that where defendant was advised of his right to remain silent prior to grand jury testimony, such testimony, although conducted pursuant to subpoena, was not compelled within the meaning of the Fifth Amendment). Thus, the Court will not suppress defendant’s response and the evidence resulting from the subsequent search on that ground.

## 2. Testimony in Violation of *Miranda*

Pursuant to *Miranda v. Arizona*, because of the inherently coercive nature of custodial interrogations, a person must be advised of his or her constitutional rights – including the right to an attorney and the right to remain silent – prior to questioning. 384 U.S. 436, 444 (1966). “As noted above, the Fifth Amendment prohibits use by the prosecution in its case in chief only of *compelled* testimony.” *Oregon v. Elstad*, 470 U.S. 298, 307 (1985). However, “[t]he *Miranda* exclusionary rule . . . serves the Fifth Amendment and sweeps more broadly than the Fifth Amendment itself. It may be triggered even in the absence of a Fifth Amendment Violation.” *Id.* at 306.

*Miranda*’s protections apply when the government subjects an individual in custody to an interrogation. *United States v. Kim*, 292 F.3d 969, 973 (9th Cir. 2002). It is undisputed that defendant was in custody for the purposes of *Miranda* at the time that she provided the passcode to her cellphone. Early in the morning on April 12, 2018, officers arrested, handcuffed, and searched defendant and transported her to the federal courthouse in a law enforcement vehicle. (See Ferrer OIG Memo at MJM-0843.) From the time of her arrest at approximately 7:00 a.m.

1 until SA Collins approached defendant to obtain the passcodes to the phones found in defendant's  
2 residence around 11:40 a.m., defendant was subject to the continuous control of state officers,  
3 federal agents, and the U.S. Marshals. (*Id.*)

4 It is also undisputed that SA Collins' statement "inform[ing] [defendant] that he was there  
5 to get the passcodes for the phones" constitutes an interrogation for the purposes of *Miranda*. See  
6 *Rhode Island v. Innis*, 446 U.S. 291, 301 (1980) (holding that for the purposes of *Miranda*, an  
7 interrogation refers not only to "express questioning" but also to its functional equivalent, which is  
8 "any words or actions on the part of the police (other than those normally attendant to arrest and  
9 custody) that the police should know are reasonably likely to elicit an incriminating response from  
10 the subject"). Accordingly, law enforcement officers were required to provide *Miranda* warnings  
11 prior to Collins' interrogation of defendant. The record reflects that officers informed defendant  
12 of her *Miranda* rights, including her right to counsel, at the time of her arrest. (See Ferrer OIG  
13 Memo at MJM-0843); see also Motion at 11.)

14 "The right to counsel recognized in *Miranda* is sufficiently important to suspects in  
15 criminal investigations . . . that it requires the special protection of the knowing and intelligent  
16 waiver standard." *Davis v. United States*, 512 U.S. 452, 458 (1994) (internal quotations and  
17 citations omitted). "If a suspect effectively waives his right to counsel after receiving the *Miranda*  
18 warnings, law enforcement officers are free to question him. But if a suspect requests counsel at  
19 any time during the interview, he is not subject to further questioning until a lawyer has been  
20 made available or the suspect himself reinitiates conversation." *Id.* (internal citations omitted). In  
21 order to invoke the right to an attorney, a suspect must unambiguously assert his or her right to  
22 counsel. *Id.* at 459 (holding that suspects statement "Maybe I should talk to a lawyer" was not an  
23 unambiguous request for counsel). Once a suspect has so invoked, he or she cannot be questioned  
24 regarding any offense unless an attorney is actually present. *Minnick v. Mississippi*, 498 U.S. 146,  
25 151 (1990).

26 As noted above, after the officers informed defendant of her *Miranda* rights, she  
27 "requested to contact her attorney, Paula Canny." (Collins OIG Memo at MJM-849.) Such a  
28 request constitutes unequivocal invocation of her right to counsel. See *Sessoms v. Grounds*, 776

F.3d 615, 626 (9th Cir. 2015) (finding that where suspect “was deferentially asking whether he could have a lawyer” he unequivocally requested counsel) (citing *United States v. Lee*, 413 F.3d 622, 625 (7th Cir. 2005) (recognizing defendant’s statement “[c]an I have a lawyer?” as an unequivocal request for counsel); *United States v. Hunter*, 708 F.3d 938, 948 (7th Cir. 2013) (holding that “[c]an you call my attorney?” was an unequivocal request for counsel)).

For the reasons stated herein, SA Collins’ statement to defendant that “he was there to get the passcodes for the phones[,]” after she had unequivocally invoked her right to counsel, violated defendant’s *Miranda* rights and thus, her provision of her passcode and any evidence subsequently derived is subject to suppression. However, “the *Miranda* presumption, though irrebuttable for the purposes of the prosecution’s case in chief, does not require that the statements and their fruits be discarded as inherently tainted. Despite the fact that patently voluntary statements taken in violation of *Miranda* must be excluded from the prosecution’s case, the presumption of coercion does not bar their use for impeachment purposes.” *Oregon*, 470 U.S. at 298; *see also United States v. Gomez*, 725 F.3d 1121, 1126 (9th Cir. 2013).

In determining whether an individual made a statement voluntarily, despite violations of *Miranda*, “the finder of fact must examine the surrounding circumstances and the entire course of police conduct with respect to the suspect in evaluating the voluntariness of his [or her] statements. The fact that a suspect chooses to speak after being informed of his [or her] right is, of course, highly probative.” *Oregon*, 470 U.S. at 318. “The due process voluntariness test takes into account the totality of the circumstances to examine ‘whether a defendant’s will was overborne by the circumstances surrounding’” the statement. *United States v. Gamez*, 301 F.3d 1138, 1144 (9th Cir. 2002) (quoting *Dickerson v. United States*, 530 U.S. 428, 434 (2000)). “Thus, the prosecution must prove by at least a preponderance of the evidence that the confession was voluntary.” *Lego v. Twomey*, 404 U.S. 477, 489 (1972).

The due process voluntariness test bears a striking resemblance to that for compulsion under the Fifth Amendment, discussed herein. *Compare Gamez*, 301 F.3d at 1144 (“whether a defendant’s will was overborn by the circumstances”) (internal quotations omitted) *with Washington*, 431 U.S. at 188 (“whether, considering the totality of the circumstances, the free will

of the witness was overborne”). As the Court previously found, the circumstances surrounding SA Collins’ statement to defendant that “he was there to get the passcodes for the phones” do not rise to the level required to have overborne defendant’s free will. *See supra*, II.B.1.c. Thus, the Court found that defendant provided her cellphone passcode voluntarily. *See id.*; *Gamez*, 301 F.3d at 1144; *see also United States v. Hernandez*, No. 18-CR-1888-L, 2018 WL 3862017, at \*3-5 (S.D. Cal. Aug. 13, 2018) (finding that even if defendant’s “demonstration of her square pattern [cellphone] passcode” qualifies as testimonial for the purposes of *Miranda*, “the conditions surrounding [d]efendant’s interrogation [following her arrest at the border for drug trafficking] do not demonstrate the kind of psychological or physical duress needed to show involuntariness”). Accordingly, the government may use, for impeachment purposes only, defendant’s statement of her passcode, the search of her cellphone, and the evidence resulting from that search. *See Oregon*, 470 U.S. at 298.

### C. The Sixth Amendment

The Sixth Amendment guarantees that “in all criminal prosecutions, the accused shall enjoy the right . . . to have the Assistance of Counsel for his defense.” U.S. Const. amend. VI. The right to counsel attaches when the “government . . . use[s] the judicial machinery to signal a commitment to prosecute” such that the “suspect” becomes the “accused.” *Rothgery v. Gillespie County*, 554 U.S. 191, 211 (2008). Suspects are thus entitled to the help of an attorney once the government has initiated formal proceedings, “whether by way of formal charge, preliminary hearing, indictment, information, or arraignment.” *Brewer v. Williams*, 430 U.S. 387, 415 (1977).

Defendant’s Sixth Amendment right to counsel attached once the government initiated formal proceedings against her by way of criminal complaint on April 9, 2018. *See* Dkt. No. 1; *see also Brewer*, 430 U.S. at 415 (noting that a “formal charge” triggers Sixth Amendment protection). Moreover, approximately an hour prior to SA Collins and SA Ptaszek visiting defendant in the Marshals holding cell for the purpose of obtaining passcode to her cellphone, defendant made her initial appearance, during which the court provisionally appointed Assistant Federal Public Defender Jodi Linker to represent her. *See* Dkt. No. 3; OIG Memo at MJM-849; *see also Brewer*, 430 U.S. at 415 (noting that a “preliminary hearing” triggers Sixth Amendment



Protection).

“[O]nce adversary proceedings have commenced against an individual, he [or she] has a right to legal representation when the government interrogates him [or her].” *Brewer*, 430 U.S. at 415. Such interrogation occurs when the government acts in a way to “deliberately elicit” incriminating information in the absence of counsel. *Massiah v. United States*, 377 U.S. 201, 204 (1964). The government need not engage in explicit questioning to trigger Sixth Amendment protections—a defendant may demonstrate interrogation where law enforcement “takes some action . . . that was designed deliberately to elicit incriminating remarks.” *See Kuhlmann v. Wilson*, 477 U.S. 436, 459 (1986). SA Collins’ statement to defendant that “he was there to get the passcodes for the phones” constitutes such an action. *See Brewer*, 430 U.S. at 401-402 (holding that where legal proceedings had commenced against a criminal defendant and detective made statements intended to obtain incriminating information, the detective violated the defendant’s right to counsel). Moreover, and as noted above, defendant had unequivocally invoked her right to counsel in SA Collins’ presence prior to their arrival at the federal courthouse. *See supra*, III.B.2.

Therefore, the Court finds that by approaching defendant after the initiation of formal proceedings, and after defendant had unequivocally invoked her right to counsel, and stating “that he was there to get the passcode for the phones[,]” SA Collins violated defendant’s Sixth Amendment right to counsel. Accordingly, the Court will suppress defendant’s statement regarding the passcode to her cellphone, the resulting search of her phone, and all evidence subsequently derived from that search.


### III. CONCLUSION

Thus, the Court **GRANTS** defendant’s motion to suppress her statement regarding the passcode to her cellphone, the resulting search of her phone, and all evidence subsequently derived from that search as obtained in violation of defendant’s Fourth and Sixth Amendment rights, as well as her rights under *Miranda*.<sup>6</sup>

---

<sup>6</sup> The Court is unpersuaded by the government’s assertion during oral argument that law enforcement would have inevitably discovered the evidence contained on defendant’s cellphone

**IT IS SO ORDERED.**

  
YVONNE GONZALEZ ROGERS  
UNITED STATES DISTRICT COURT JUDGE

because the cellphone itself “was seized pursuant to a valid warrant” and that the evidence is, therefore, not subject to suppression. Although the government failed to raise this issue in its brief, it seems that the facts of this case suggest that discovery of the contents of defendant’s cellphone, identified as evidence item SIRGM2, was not inevitable without law enforcement obtaining defendant’s passcode. SMPD previously seized and obtained a warrant for search of a cellphone belonging to defendant. (*See* SMPD Report at MJM-545; SM Warrant at MJM-561.) Defendant initially refused to provide the passcode for her locked iPhone, and even after she did so provide, once the forensic analyst for SMPD examined the phone, someone had “wiped” the device, such that law enforcement could not obtain any evidence therefrom. (Aff. in Sup. Fed. Compl. ¶ 65; SMPD Suppl. Report at MJM-5325.)